

ADSS Server v4.5.5 Release Notes



This document provides a high-level description of the new features offered in each release of ADSS Server. Only the main features in each release are identified.

ADSS Server v4.5.5

April 2012

- ADSS TSA Service now supports Microsoft Authenticode timestamp requests.
- ADSS Signing Service now supports PDF Permissions and can thus set copying, printing and commenting rights. The signature appearances designer has been enhanced to allow much greater control of signature appearances for new or existing signature fields.
- ADSS CRL Monitor has been enhanced to factor the CRL freshness policy into the calculation of when the CRL Next Update time has arrived. There is also a new option that allows just the latest CRL to be retained to improve database size management for one or multiple CAs with very large CRLs. The Transaction Log viewer has been enhanced.
- ADSS Trust Manager has been enhanced to enable a Time Stamp Authority to be associated with a particular CA so that local signatures can be extended using the appropriate TSA when using a common signature profile.
- The ADSS Console starts quicker than before with any alerts shown after the home page has loaded.

ADSS Server v4.5.4.2

March 2012

- Certificate path building has been enhanced in various ADSS services to support non-English characters in certificate subject name.

ADSS Server v4.5.4.1

March 2012

- Resolved an OCSP service issue related to loading CRLs in memory for high speed OCSP responses.

ADSS Server v4.5.4

March 2012

- ADSS CRL Monitor has been enhanced to allow all prior CRLs to be deleted and thus reset CRL information for a particular CA.
- ADSS CRL Monitor can now import revocation information from multiple partitioned CRLs stored in an LDAP repository as a feed for the OCSP service.
- ADSS LTANS Service has been enhanced such that (a) LTANS profiles now define the Signing and Verification authority addresses to be used and (b) greater control is offered over the inclusion of meta-items when computing the XMLERS and notary signatures and during subsequent storage.
- ADSS Signing and Verification services now support PDF collections.
- The ADSS Signing Service PDF signature appearances designer has been improved.
- Following a successful ETSI PAdES plug test a number of enhancements have been integrated.
- The Certification Service now supports the deletion of valid keys and certificates via the API.
- PostgreSQL 9.1 has been tested and added to the list of supported databases.
- Solaris 11 has been tested and added to the list of supported operating system.

ADSS Server v4.5.3.3

February 2012

- Resolved a CRL Monitoring issue related to CRL polling.

ADSS Server v4.5.3.2

February 2012

- Resolved an issue related to XML signature verification in ADSS Verification Service.
- ADSS Server installation wizard has been enhanced to resolve a problem with inserting sample data

ADSS Server v4.5.3.1

January 2012

- Path validation has been enhanced in XKMS, SCVP and Verification services to support dynamic path building using NIST LDAP repository. PKITS test cases pass when test data is imported manually and also when data is discovered dynamically from NIST LDAP repository.

ADSS Server v4.5.3

January 2012

- The ADSS Signing service higher speed HTTP interface has been enhanced to support signing attributes and PDF signature appearance profiles (these were already supported within the OASIS DSS interface).
- The OCSP service and Timestamp service response messages now support signing using the GOST algorithm.
- ADSS Server has been updated to use Java EE 6 release 29 (jdk1.6.0_29).

ADSS Server v4.5.2.2

January 2012

- An issue related to database connection pool management has been resolved.

ADSS Server v4.5.2.1

November 2011

- Handling of longer key aliases is enhanced for the keys imported from hardware crypto devices.

ADSS Server v4.5.2

November 2011

- To respond to the recent attacks on trusted CA services ADSS Server can be licensed to enable Trust Manager to mark a CA as revoked so that all signature and certificate validation requests receive revoked responses for any issued certificate. Also CRL Monitor now allows individual certificates to be marked as revoked to allow a fraudulent certificate that was not legitimately issued to be treated as revoked.
- The Certification Service has been enhanced to allow an option to set the "Valid From" date/time for a new certificate to be in the future.
- The OCSP Service has been updated to provide an option to check if a good target certificate (i.e. not identified within a CRL) was actually issued by the issuing CA (only if the ADSS Local CA was the certificate issuer).

ADSS Server v4.5.1.3

February 2012

- Path discovery has been enhanced in XKMS, SCVP and Verification services to avoid manually configuring additional LDAP repositories and CRLs for Trust Anchor certificates.

ADSS Server v4.5.1.2

January 2012

- Path validation has been enhanced in XKMS, SCVP and Verification services to support dynamic path building using NIST LDAP repository. PKITS test cases pass when test data is imported manually and also when data is discovered dynamically from NIST LDAP repository.

ADSS Server v4.5.1

October 2011

- The Verification Service has new options when checking a long-term signature that does not have an embedded timestamp: (a) the signature can be checked at the current time, or (b) an error can be returned.
- The Signing, Verification, XKMS, LTANS, Certification and Decryption Services now allow profiles to be referenced by Profile Name as well as by Profile Id.
- The OCSP Service has been updated to allow the OCSP response signature to include its certificate alone or the full certificate chain.
- The Signing Service now allows signature appearances to be overridden if this option is enabled.

ADSS Server v4.5.0.2

October 2011

- The HSM automatic reconnection feature has been enhanced.

ADSS Server v4.5.0.1

October 2011

- An issue related to database connection pool management has been resolved.
- Handling of revoked target certificates is enhanced in the ADSS XKMS Service.

ADSS Server v4.5

August 2011

- Support for the Russian GOST algorithm has been added.
- Support for reason based segmented CRLs has been added.
- Certificate validation has been enhanced within the SCVP, XKMS and Verification services to include:
 - a) LDAP referrals are now supported in DPD (Delegated Path Discovery);
 - b) Indirect CRLs support is enhanced to satisfy PKITS DPV and DPD test cases;
 - c) Information on non-registered CAs and their CRLs found within DPD processing is now cached.

ADSS Server v4.4.4.2 (Patch release)

August 2011

- An issue related to signing PDF on multiple pages has been resolved.

ADSS Server v4.4.4.1 (Patch release)

August 2011

- HSM auto reconnection logic has been enhanced.

ADSS Server v4.4.4

July 2011

- The ADSS Signing Service can now use configuration settings to manually allocate and optimise the space for PDF signature dictionaries.
- The Certification Service and Manage CAs modules now support custom Subject Alternative Name and Issuer Alternative Name extensions and the Manage CAs module can now publish CRLs to an LDAP directory.
- The transaction logs viewer in the Verification, XKMS and SCVP service modules now provides full details of an expired CRL within the signer certificate chain.
- The ADSS Server console now automatically connects to multiple load balanced ADSS Server instances.

ADSS Server v4.4.3

June 2011

- The performance of ADSS Server Delegated Path Discovery (DPD) has been substantially increased and timeout values in seconds can now be set.
- ADSS SCVP Service now supports an easy to understand structured view of the SCVP request and response messages.
- Certificate distinguished name default configurations have been moved from Global Settings to the Key Manager module.
- A separate support utility has been added that can be used to verify the full functionality of a PKCS#11 HSM device during interop testing or fault finding.

ADSS Server v4.4.2.1 (Patch release)

June 2011

- An ADSS Verification Service long term signature verification issue has been fixed as has a key quality issue when verifying PDF signatures.
- The ADSS Signing service has been enhanced by extending support for detached PAdES signatures according to ETSI TS 102 778 V1.1.1 (2009-07) PAdES profiles.

ADSS Server v4.4.2

May 2011

- ADSS Signing Service has been enhanced by:
 - (a) Supporting "ISO 8601" date formats in PDF Signature appearance;
 - (b) Extending support for special language characters;

- (c) Providing new settings, that can prevent a label with no value being shown for a PDF signature field when no value is supplied, e.g. (Reason: /Location: /Contact:).
- ADSS Signing and Verification services have been enhanced by providing support to generate and verify counter signatures.
- ADSS Verification Service has been enhanced by adding support for enhancing the PAdES signatures to part 3 and part 4.
- Added support for “CRL Entry Extensions” within OCSP response messages.
- SHA2 and RipeMD hashing algorithms are now supported ADSS CA Service CRL publishing.
- The ADSS TSA Service has been enhanced by:
 - (a) Adding an allowed hash algorithm list;
 - (b) Adding an option to reject a TSA request if it does not contain the 'certReq' flag.
- ADSS SCVP Service has been enhanced to support further RFC 5055 options, e.g. scvpServer and scvpClient EKUs are now supported in request / response signing certificates respectively.
- NTP time monitoring has been enhanced to generate an alert and stop ADSS Services when none of the configured NTP servers can be connected.
- Added support to generate certificates with multiple RDNs.

ADSS Server v4.3.4 (Patch release)	May 2011
---	-----------------

- An ADSS SCVP Service path verification issue with Self-Issued certificates has been fixed.
- An ADSS Verification Service long term signature verification issue has been fixed. Also resolved an XML verification issue when the signer is revoked.

ADSS Server v4.3.3 (Patch release)	April 2011
---	-------------------

- An ADSS SCVP Service FPKI path building issue has been fixed.
- An ADSS Verification Service long-term signature issue has been fixed.

ADSS Server v4.3.2 (Patch release)	April 2011
---	-------------------

- The ADSS TSA Service now supports a list of allowed algorithms.
- An ADSS Signing Service issue relating to the handling of images within signature appearance profiles has been fixed.
- An upgrade issue relating to the default HMAC key has been resolved.

ADSS Server v4.3.1 (Patch release)	March 2011
---	-------------------

- Resolved a trust chain issue affecting OCSP Service start-up.
- Resolved a location issue relating to blank signature field creation.
- Resolved an issue relating to email address parsing.

ADSS Server v4.3	February 2011
-------------------------	----------------------

- ADSS Signing and Verification services have been enhanced by:
 - (a) Providing support for PAdES signatures based on ETSI PAdES standard (TS 102 778);
 - (b) Providing extended support for XAdES and CAdES specifications;
 - (c) Supporting the creation of PDF signature fields using X/Y coordinates (OASIS DSS-X profile).
- ADSS Signing, Verification, XKMS, Certification and LTANS services have been extended to support SOAP v1.2.
- ADSS Verification and XKMS services have been enhanced to support enveloping XML signatures in request and response messages. The ADSS XKMS Service additionally supports detached XML signatures in request and response messages.
- ADSS Verification, SCVP and XKMS services have been extended to support PKITS compliant path discovery and path validation. The Verification and XKMS services have also been enhanced to extend support for detailed PEPPOL requirements.
- A new ADSS Verification Gateway Service has been introduced as a licensed option within ADSS Server. This new service replaces the original ADSS Gateway software. Managed

service providers need such Verification Gateways to allow clients to protect their data privacy by extracting the document signatures and sending only these for external verification.

- The ADSS TSA Service has been enhanced to support ESSCertIDv2 Update for RFC 3161.
- A new time drift check facility allows ADSS Server to check that server system time is acceptably accurate by cross-checking with a list of trusted NTP servers. If predefined thresholds are exceeded then ADSS Server (a) warns operators about the unacceptable time drift and can then (b) stop all services.
- ADSS Server home screen alerts have been enhanced such that the hyperlink only shows those records which are relevant to the specific alert.
- Management reports have been added to the XKMS, SCVP and LTANS service modules which provide different levels of graphical and tabular reports on service usage in real-time. Reports can be exported in PDF format or as CSV files.
- The ADSS Server installation wizard now installs three different ADSS Server components, namely (a) the Core service, (b) the Console service and (c) selected Service modules. Each of these components uses a separate Java Virtual Machine to provide better resource management for high performance systems. Administrators can choose to install these components on just one single system or on separate physical or virtual machines.
- The ADSS Trust Manager module has been enhanced in these ways:
 - (a) When deleting a CA, if the CA is used elsewhere then the references to it are shown so that an administrator can confirm or cancel the delete request;
 - (b) Validation policy configurations can now allow the real-time downloading and caching of CRLs and use them to validate certificates issued by a registered CA – this is particularly relevant when checking certificates issued by Entrust CAs that feature partitioned CRLs;
 - (c) When registering a new CA the Friendly Name offered uses CA certificate common name by default to save time and mistakes - the default value can be used or changed as required;
 - (d) When adding CRL resource addresses for a CA, a certificate it has issued can be identified so that all the CDP addresses are automatically read and added to the CRL resource list - this saves operator time and prevents typing mistakes;
 - (e) A hierarchal view of registered CA certificates is now provided that shows chained certificates in a tree structure. The old classic view is still available if required.
- When deleting a key within Key Manager, if the key is used anywhere within the ADSS Server, the references to it are shown so that an administrator can confirm or cancel the delete request.
- CRL Monitor now allows the administrator to manually update a CRL without first turning off CRL polling within Trust Manager – this saves operator time when configuring a system.
- Wild card search is now available in various ADSS Server modules.

ADSS Server v4.2.9 (Patch release)	February 2011
------------------------------------	---------------

- Resolved an issue relating to external Time Stamping Authorities with a space in their DName.

ADSS Server v4.2.8 (Patch release)	January 2011
------------------------------------	--------------

- Support for ECDSA has been added to meet FIPS201 requirements.
- HMAC computation has been enhanced to handle network HSM disconnections.

ADSS Server v4.2.7 (Patch release)	December 2010
------------------------------------	---------------

- The Key Manager HSM connection test has been enhanced.
- The System Log Viewer has been enhanced. It now shows a Log ID column in the Operational Logs and an issue with importing archived logs has been fixed.
- XAdES/CAAdES plug test enhancements have been integrated.

ADSS Server v4.2.6 (Patch release)	November 2010
------------------------------------	---------------

- Key Manager key importing has been enhanced.

ADSS Server v4.2.5 (Patch release)	October 2010
------------------------------------	--------------

- Resolved a CRL Monitor issue associated with CRL 'certificateHold' entries that have no 'holdInstructionCode'.

ADSS Server v4.2.4 (Patch release)	October 2010
---	---------------------

- Resolved a CRL Monitor issue with handling delta CRLs.
- Resolved a Verification, XKMS and SCVP services PKIX validation issue.
- Improved the way Key Manager displays certificate templates and imports PFX/PKCS#12 files.

ADSS Server v4.2.3 (Patch release)	September 2010
---	-----------------------

- The ADSS Verification Service has been extended to support an additional OASIS DSS VerifyInfo attribute "Id".
- Resolved an issue with the loading of historic CRLs in ADSS Verification Service.

ADSS Server v4.2.2 (Patch release)	September 2010
---	-----------------------

- Resolved an issue in Verification service profile handling.
- Resolved an issue with CRL Monitor email alerting when polling for multiple CRL addresses.
- Resolved an issue with headless installation on non-Windows platforms.

ADSS Server v4.2.1 (Patch release)	August 2010
---	--------------------

- The ADSS SCVP Service has been extended to meet the GSA FIPS 201 test case requirements.
- The PKIX implementation has been extended in the XKMS, SCVP and signature verification services to meet more of the PKITS test cases.

ADSS Server v4.2	July 2010
-------------------------	------------------

- The ADSS Signing Service now includes support for signed attributes in CAAdES and XAdES signatures as an option during OASIS DSS signing operations. Signing profiles now allow a signature grace period to be configured which defines how long the ADSS Server should wait after the signing time (shown in the timestamp or otherwise the signer's local system time) before converting the basic signature to an advanced ETSI AdES signature.
- The ADSS Verification Service has been extended to support additional DSS-X verification reports, such as returning authenticated and unauthenticated attributes and the verification of the full chain for CRLs and OCSP responder certificates. In addition the Verification Service profiles have been extended to support signature grace periods. These define how long the ADSS Server should wait after the signing time (shown in the timestamp or otherwise the signer's local system time) before verifying a signature. PEPPOL optional inputs are now supported as is the configuration of a peer XKMS server to determine revocation information for certificates whose issuer is not locally trusted on ADSS Server.
- The ADSS XKMS Service has been extended to support PEPPOL extensions. XKMS Service profiles have been introduced to allow greater granularity of the configuration options in such areas as Trust Anchors and certificate validation options. The transaction logging has also been enhanced for better presentation of the certificate validation process information.
- The ADSS SCVP Service has been extended to support Delegated Path Validation (DPV) with optional validation policy attributes in the response & support for multiple certificates in a request.
- The ADSS Verification, XKMS and SCVP services now support these features:
 - (a) PKIX algorithm based validation of the certificate chains;
 - (b) Transaction logging has been enhanced to also store the validation profile configuration at the time of verification to allow a later audit review of the ADSS Server decisions.
- The ADSS OCSP Service has a new feature to allow high speed OCSP response processing by optionally not storing the OCSP transactions and caching the latest CRL in memory.
- The number of internal ADSS Server "local CAs" has been extended. A new ADSS Server "Manage CAs" module has been created to allow multiple Root and issuer CAs to be configured if required. Configuration for all local and external CAs has been moved to "Manage CAs".

- A new alerting system has been introduced to display alerts on the ADSS Server home page for various events such as license expiry, certificate expiry (includes CAs, clients and end user certificates), unused service profiles and uncertified keys within the Key Manager.
- The ADSS Access Control module has been enhanced to allow greater control over operator roles. Each service module and its sub-modules can be controlled whether to allow Add, Delete, or Modify operations and enabling dual control is now possible at a sub-module level.
- All ADSS Server services can now be configured to retry connections with external OCSP, TSA and CRL addresses when there is a connection failure.
- The ADSS Server Global Settings module has been enhanced to support client authentication when communicating with a TSA Server running over SSL with client authentication.

ADSS Server v4.1.4 (Patch release)	June 2010
---	------------------

- Resolved an issue with SNMP alerting to include ADSS Server IP address.

ADSS Server v4.1.3 (Patch release)	June 2010
---	------------------

- Resolved an issue with handling Unicode characters within the signature appearance designer.
- Resolved an issue with repeated optional output elements within DSS verification response.

ADSS Server v4.1.2 (Patch release)	May 2010
---	-----------------

- Enhanced the proxy handler to support NTLM authentication.
- Enhanced the PDF signature appearance designer to allow signature labels to be modified.
- Resolved an issue with handling remote file paths within LTANS service request messages.

ADSS Server v4.1.1 (Patch release)	May 2010
---	-----------------

- Fixed an issue with handling Operator CA certificates that contain a quotation character.
- Fixed an issue related to terminating the ADSS Server process when stopping on Unix platforms.
- Fixed an issue with creating signed and timestamped Verification Service response messages.

ADSS Server v4.1	April 2010
-------------------------	-------------------

- The ADSS Signing Service has been extended to support the enhancement of basic signatures to more advanced ETSI AdES formats as an option during OASIS DSS signing operations. In addition signature appearance attributes are now supported in the signing request as defined in the OASIS DSS-X Visible Signatures profile. Signing profiles now allow even greater configuration flexibility including the option to select alternate signing keys/certificates – this is valuable when load balanced servers need to sign using a key/certificate held within their own local PCI HSM where cloning of HSM keys and certificates is not allowed by the trust scheme, e.g. Adobe CDS Certificates.
- The ADSS Verification Service has been extended to support the enhancement of basic signatures to more advanced ETSI AdES formats as an option during OASIS DSS verification operations. OASIS DSS-X Verification Reports are supported and PEPPOL trust ratings are now available to determine signature and certificate quality. The Verification Service profiles have been extended to allow greater granularity of the configuration options in such areas as Trust Anchors, signature formats and certificate validation options. CRLs can now be optionally retrieved in real-time from the CDP contained in the target certificate – useful for partial CRLs. Finally the transaction logging has been enhanced for better presentation of the signature verification and certificate validation process information.
- The ADSS TSA Services has been extended to support RipeMD160 and SHA 224 hash algorithms. A new option is provided to use the HSM internal time clock when generating timestamp tokens provided this is supported by the target hardware.
- The ADSS LTANS Service has been extended to include a range of new features such as:
 - (a) supporting application supplied meta data attributes within the generated evidence record;
 - (b) searching meta data attributes to select evidence records;
 - (c) return XMLERS data back if requested within export transactions;
 - (d) verify archived evidence records before they are returned in export transactions;
 - (e) able to select whether to store the original data within the archive, file system or to post to a

- configured URL and allowing the option to only store the evidence record and not the data;
- (f) archive profiles can configure how to verify signed data objects before they are archived;
- (g) archive profiles can control the deletion policy for archived information;
- (h) Support is provided to read and write large data objects via network paths.

- A new ADSS SCVP Service is now available as a licensed option. This follows the recently ratified RFC 5055 Server-based Certificate Validation Protocol standard. Delegated Path Validation (DPV) has been implemented in this release.
- The ADSS OCSP Service has been enhanced to support real-time revocation information for the local ADSS Server CA and support additional hash algorithms.
- The ADSS CRL Monitor service has been enhanced to be able to optionally monitor and check all CRL resources for a defined CA. Alerts can be sent if any of the CRL resources are seen to have trust issues within them. Delta CRLs are now also supported.
- Within all ADSS Server services the transactions log viewer screens have been enhanced to allow operators to select which columns they wish to show on the screen. Extended character set certificates and CRLs can now be used within ADSS Server. SNMP (Simple Network Management Protocol) based alerts are also now available.

ADSS Server v4.0.4 (Patch release)	March 2010
---	-------------------

- Added msvcr71.dll redistributable to avoid ADSS Server Windows service startup problems. This avoids operators having to copy this DLL manually.

ADSS Server v4.0.3 (Patch release)	March 2010
---	-------------------

- PKCS#11 enhancements have been made to better handle existing keys and certificates.
- Certificate templates now use an updated country list.
- Oracle 11g has been added to the list of supported databases.
- The ADSS LTANS Service has been enhanced to better handle the evidence renewal process
- Fixed a bug relating to external Time stamping Authorities with a space in their DName.

ADSS Server v4.0.2 (Patch release)	February 2010
---	----------------------

- Enhanced the HMAC feature to work with a broader range of HSMs.
- Enhanced the policy controls for CRL based validation in the signature verification service.
- The Certification Service can now use the full PKCS#10 subject DN attributes.
- CRL handling within the Trust Manager and the CRL Monitor service has been enhanced.
- CRL Monitor now supports digest authentication when downloading CRLs for configured CAs.
- Stale connections to a MySQL database are now automatically recovered.

ADSS Server v4.0.1 (Patch release)	January 2010
---	---------------------

- The ADSS Server certificate viewer now supports Qualified Certificate statement extension details.
- Navigation on the ADSS Server Global Settings > Certificate Templates page has been enhanced.
- Indirect CRLs resources can now be successfully tested from within the ADSS Trust Manager when registering a CA.
- The optional sample test data that can be used at installation time has been enhanced.

ADSS Server v4.0	November 2009
-------------------------	----------------------

- Added the following features as part of the CEN CWA 14167-1 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements) compliancy audit:
 - Check the expiry of certificate before use in any ADSS service (e.g. Signing, Verification, Certification, TSA, OCSP etc.)
 - Perform revocation checking for back-end SSL/TLS server authentication certificates, ADSS infrastructure certificates and back-end TSA certificates.

- Ability to issue emergency CRLs at the time of receiving a revocation request within ADSS Certification Service.
 - Support for IETF CMC protocol for processing certificate generation and certificate revocation requests from CMC-compliant clients, e.g. RA systems like AET BlueX. CMC over SSL/TLS is also supported for client authentication.
 - Ability to terminate the SSL session upon log out or session timeout; in both the cases operator needs to re-launch the ADSS Server console in a new browser instance in order to re-login to ADSS Server.
 - Support the generation of the ADSS Server Tomcat SSL Server Authentication key inside PKCS#11 devices e.g. HSM.
 - Support the generation of system integrity checking HMAC keys in PKCS#11 devices e.g. HSM, Also included the ability to update the HMAC key.
 - Dual control facility is extended within Approval Manager to also cover generation/import of keys in Key Manager and import of configurations in the Global Settings module.
 - Provides a built-in certificate viewer capable of showing the certificate's fingerprint and the related fingerprint algorithm.
 - Support for ETSI Qualified Certificate profile (TS 101 862) within the ADSS Certification Service module. A built-in certificate profile template is added for this purpose.
 - Ability for administrators to enable Tomcat's SSL debug logging to record login failures attempts performed by ADSS operators.
- The Certification Service module now supports manual certification by importing an external PKCS#10/CSR (certificate signing request) and issue certificate against the imported PKCS#10.
 - The Certification Service module now supports creation of new certificate templates in addition to the default ones.
 - ADSS Server can now be installed in headless mode i.e. without a GUI-based wizard. This option is provided to help administrators to remotely install ADSS Server on non-Windows machines.

ADSS Server v3.8.1 (Patch release)	November 2009
---	----------------------

- Improved auto-upgrade facility when upgrading from previous releases of the ADSS Server.
- Resolved an issue related to HMAC verification.

ADSS Server v3.8	October 2009
-------------------------	---------------------

- The Signing Service now supports CAdES-C, XAdES-C and XAdES-X type2 signature formats.
- The Signing Service can now accept basic signatures and enhance them by embedding timestamp and certificate status information using the relevant PDF, CAdES and XAdES profiles.
- The Signing Service now supports the production of German SigG standard compliant signatures using RipeMD160 hash and RSA 1024 keys in conjunction with services from www.SignTrust.de.
- ADSS GoSign Applet now supports local hashing. GoSign Professional is now available and provides licensed options for PDF viewing, timestamped and long-term signature support. GoSign Applet functionality is now controlled by use of a license.xml file.
- The Certification Service now supports roaming credentials. These credentials generated by ADSS GoSign Applet and are stored within a secure container on the ADSS Server. They are delivered to users needing to sign a document within the new ADSS GoSign Professional applet.
- The XKMS Service module can now return certificate status information for the full certificate chain of the target certificate, OCSP responder and the CRL issuer certificates within a single request/response call.
- A controlled option is available to support the decryption of XML documents using an OASIS DSS-X Encryption Profile compliant Decryption Service module. The encryption of the target data within an XML structure is possible using a special licensed option of the ADSS GoSign Professional Applet - ask for further details.

ADSS Server v3.7.3 (Patch release)	October 2009
---	---------------------

- Resolved an issue in Certification Service module when configuring local CA.

ADSS Server v3.7.2 (Patch release)	September 2009
---	-----------------------

- Resolved an issue in Trust Manager to allow the use of validation policy OCSP then NONE.

ADSS Server v3.7.1 (Patch release)	August 2009
---	--------------------

- Resolved an issue in the OCSP Service module when handling suspended certificates.

ADSS Server v3.7	August 2009
-------------------------	--------------------

- ADSS Server can now accept and process one or more hash values within ADSS Signing Service using the OASIS DSS protocol. Thus client applications do not need to send whole PDF documents for signing. This increases performance substantially for large PDF documents. To support this feature the ADSS Client SDK has been updated to provide local hashing and signature object embedding for PDF documents.
- ADSS Signing Service now supports the use of authorisation profiles. These require one or more end users to sign an authorisation control file requesting that one or more documents be signed with a server-held signing key. This is useful in high-trust workflows where important documents need to be signed by a Qualified Certificate or CDS Certificate. An audit trail of approvers is created, checked and available as audit or compliance evidence. An M of N scheme is implemented to ensure business workflow flexibility.
- Updated Tomcat & JRE versions. ADSS Server now uses Tomcat 6.0.18 and JRE 1.6.0_13.
- The list of supported hash algorithms has been extended to include RipeMD128 and RipeMD160. These are needed to work with German SigG compliant signature service providers.
- The TSA Service has markedly better performance as a result of lower-overhead logging.
- A real-time certificate status checking feature has been added to ADSS Server. This can be configured for use with all validation i.e. OCSP, XKMS, Signing and Verification services. A special utility is provided to load real-time information from the Verizon Cybertrust UniCERT CA. Real-time information from other RAs and CAs can be integrated using this ADSS Server feature.
- New CRL Monitor alert events (using both email and SMS messages) have been added to cover circumstances when (a) the signature of a downloaded CRL cannot be verified and (b) when a downloaded CRL is not properly structured or has an incorrect format.
- CRL Monitor can now check that a CA that over-issues CRLs (e.g. creating a new CRL every three hours that is valid for 24 hours) is in fact meeting this policy. A new alert event has been created for circumstances when a CA fails to issue a CRL based on its over-issue policy - even if there is a valid CRL for that CA already present in the ADSS database.
- The CRL Monitor can now optionally publish downloaded CRLs to a local system after they are verified. This enables local CRL access for high security and high availability environments.
- HMAC recalculation for existing database records has been made optional when upgrading the ADSS Server. These are required to handle database schema changes from an older version to a new version. The process can now be run from a separate utility allowing an upgraded ADSS Server to start without interruption and with no delays.
- Added the option to configure two logging method for transactions in each ADSS Service module, to improve performance by reducing the number of database write transactions. Each service now has a specific configuration file for low-level system settings.
- Added a configuration option to enable the use of FIPS mode for HSMs and to enable the storage of generated certificates on to a PKCS#11 device (e.g. smartcard / USB token / HSM).

ADSS Server v3.6.3 (Patch release)	June 2009
---	------------------

- Added support to generate asymmetric key pairs and subsequent PFX files within the ADSS Certification Service without the client application having to provide the password for the PFX file in the request message. A random password is generated automatically by the ADSS Server.
- Added support for the client application to retrieve the private key file (PFX) and the associated password from the ADSS Certification Service.

ADSS Server v3.6.2 (Patch release)	May 2009
---	-----------------

- Resolved a limitation in the Key Manager to handle longer key aliases.
- Resolved an issue regarding verification of XAdES-EPES signatures.

ADSS Server v3.6.1 (Patch release)	May 2009
---	-----------------

- Resolved an issue with image scaling in PDF signature appearances. Also provided a new facility to adjust the hand-signature and company logo image sizes whilst designing the signature appearance.
- Resolved an issue concerning the use of keys/certificates existing within a PKCS#11 device, where the key alias contains special characters.

ADSS Server v3.6	April 2009
-------------------------	-------------------

- A new OASIS Digital Signature Services (DSS) standard service module has been added to extend the range of signing and verification options available and continue Ascertia's commitment to standards compliance.
- An IETF LTANS (Long-Term Archiving and Notary Service) module has been added to provide standards based secure archiving and notarising for business documents. This LTANS module supports the IETF XMLERS and LTAP specifications.
- A W3C compliant XKMS (XML Key Management Specifications) service module has been added to extend the range of options available for validating X509 digital certificates.
- The Signing service transaction logging is improved to store and display the signing requests sent over the fast HTTP protocol (e.g. requests received from AFP) – this matches what is currently provided for web-services signing requests.
- Within the Admin interface a new PDF signature appearance designer applet is provided to offer fine control over exactly where the signature field should be positioned and how the signature appearance should look.
- Added the ability to select fall-back Time Stamping Authorities in the ADSS Signing and LTAN services, in case the primary TSA becomes unavailable.
- Added support for the SHA-256 hashing algorithm when signing PDF documents.
- Within the ADSS Verification service it is now possible to verify digital signatures according to the time of signing indicated by the signer.
- ADSS services can now be run from different machines e.g. an OCSP service can be deployed on one machine to process OCSP requests and the CRL Manager service can be running separately to download and manage CRLs to share the work-load.
- Added support for exporting / importing of selected ADSS Server configurations settings from one ADSS Server instance to another.
- Transaction logging is improved in all ADSS services to show error message for the failed transactions in the relevant transactions log viewer page. Previously these errors were only available in the debug log files.
- Default sorting order of the lists in all ADSS server modules is changed to show the most recent record at the top.
- Upon configuring the local timestamp authority (TSA), the relevant TSA certificate is automatically registered in the Trust Manager with the purpose of trusting timestamps.
- Provided ability to mark profiles (e.g. signing profiles) as active / inactive in all ADSS services.
- Provided ability to make requests over SSL with client authentication to the back-end OCSP responders and time stamp authorities.
- Added support for multiple hashing algorithms to be used for OCSP response signing.
- Restricted the ability to start ADSS services until at least the basic configurations are made e.g. ADSS verification will start only when at least one active verification profile is present.
- Added support to generate and store key pairs on smart cards and USB tokens and also save associated certificates directly on the smart card and USB tokens (rather than the database).
- Various improvements to the ADSS console GUI.